REQUEST FOR CLEARANCE OF INFORMATION

FROM: (SUBMITTER, DIVISION, OFFICE SYMBOL)
Christine L. Moulton
Modeling and Simulation
RDER-NVM-SA

DATE:
2014/03/27

PR12656

IAW AR 360-1, Army Public Information, and AR 530-1, Operations Security (OPSEC), the attached material is submitted for document release approval.

SECTION I - DESCRIPTION

1. TITLE: Integrated Sensor Architecture (ISA) for Live Virtual Constructive (LVC) environments

2. AUTHOR(S): Christine Moulton, John Harrell, Susan Harkrider and Jared Hepp

3. INFORMATION TYPE: ☐ ABSTRACT ☐ VIEWGRAPHS ☒ PAPER ☐ SOFTWARE
☐ PRESS RELEASE ☐ WEB PAGE ☐ VIDEO ☐ CD/DVD
☐ OTHER: _____ (Please Specify)

4. REASON FOR CLEARANCE:

Purpose: SPIE Conference Conference Paper - Paper 9095-7

Location: Baltimore MD

Conference Date: 2014/05/05 Due Date: 2014/04/04

Audience: US Govt: ☒ US Contractors: ☒ Foreign Nationals ☒

External Publication Material will be published in: SPIE Conference Papers

SECTION II - INFORMATION REVIEW CHECKLIST: Please read and thoroughly reply to the following questions

(Explain all yes answers on Page 3)

1. Does this material contain:	Yes	No
a. Classified information (i,e. Top Secret, Secret, Confidential)?	☐	☒
b. Controlled information (i,e. FOUO, ITAR) or restrictive marking caveats? *(Portion mark accordingly)*	☐	☒
c. Distribution statements "B, C, D, E, or F"? *(Add statement to first page of document)*	☐	☒
d. Information addressed in a Security Classification Guide? *(If yes, identify which on page 3)*	☐	☒
e. Procurement sensitive, contract proposal or proprietary information that would prohibit release?	☐	☒
f. Information on inventions/patent applications for which patent secrecy orders have been issued?	☐	☒
g. Studies or after action reports containing advice, recommendations or lessons learned?	☐	☒
h. Fielding and/or test schedule information?	☐	☒
i. Information not previously published containing state-of-the-art or breakthrough technology?	☐	☒
j. Specific technical data revealing system vulnerabilities?	☐	☒

SECTION II - CONTINUED

k. Is release being done at the request of another organization, agency or contractor? *(If yes, identify on page 3)*	☐	☒
l. Is any information addressed in a RDP (Research Demonstration Project) or a TECD (Technology Enabled Capability Demonstration)? *(If yes, identify which on page 3)*	☐	☒

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
27 MAR 2014	**N/A**	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Integrated Sensor Architecture (ISA) for Live Virtual Constructive (LVC) Environments	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Christine L. Moulton /Susan Harkrider, John Harrell, and Jared Hepp	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
NVESD MSD, 10221 Burbeck Drive, Fort Belvoir, VA 22060	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**9**	

SECTION III - DISTRIBUTION

☒ (A) PUBLIC RELEASE-UNLIMITED

☐ (B) US GOVERNMENT AGENCIES ONLY

☐ (C) US GOVERNMENT AGENCIES & THEIR CONTRACTORS ONLY

☐ (D) DOD GOVT AND DOD CONTRACTORS ONLY

☐ (E) DOD COMPONENTS ONLY

☐ (F) NO FURTHER DISSEMINATION

NOTE: Please review security intranet page for more information. https://intranet.nvl.army.mil/security/

SECTION IV - REVIEW CERTIFICATION

MOULTON.CHRISTINE.LOWRY.1398397858 Digitally signed by MOULTON.CHRISTINE.LOWRY.1398397858 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=MOULTON.CHRISTINE.LOWRY.1398397858 Date: 2014.03.27 09:17:43 -04'00'	703-704-1342	
Author ***Printed Name, Signature and Date***	PHONE	DATE
Joseph J Dinek	4 0173	2014 03 31
Division Director / Division Deputy **Printed Name**, Signature and Date	PHONE	DATE Edits - Well Done!
JF Ball Jr	41860	4 April 14
Technical Review ***Printed Name,Signature and Date***	PHONE	DATE
		Add distribution "A" Statement
CHERYL R. BAILIE Security Specialist Cheryl R. Bailie	41149	8 Apr 14
OPSEC ***Printed Name, Signature and Date***	PHONE	DATE
KENNETH J. MCDAVID Security Manager	41173	8 Apr 14
Security Manager ***Printed Name, Signature and Date***	PHONE	DATE

SECTION V. - PUBLIC AFFAIRS OFFICER APPROVAL/DISAPPROVAL:

☑ ☐	KBell	4/9/14
APPROVED / DISAPPROVED	Document Release Officer Approval ***Printed Name,Signature and Date***	DATE

SECTION III - INFORMATION REVIEW CHECKLIST (Continuation Sheet)

Add Distribution "A" Statement

Integrated Sensor Architecture (ISA) for Live Virtual Constructive (LVC) Environments

Christine L. Moulton – Night Vision Electronic Sensors Directorate
Susan Harkrider - Night Vision Electronic Sensors Directorate
John Harrell – Oakwood Controls
Jared Hepp – Oakwood Controls

ABSTRACT

The Integrated Sensor Architecture (ISA) is an interoperability solution that allows for the sharing of information between sensors and systems in a dynamic tactical environment. The ISA created a Service Oriented Architecture (SOA) that identifies common standards and protocols which support a net-centric system of systems integration. Utilizing a common language, these systems are able to connect, publish their needs and capabilities, and interact with other systems even on disadvantaged networks. Within the ISA project, three levels of interoperability were defined and implemented and these levels were tested at many events. Extensible data models and capabilities that are scalable across multi-echelons are supported, as well as dynamic discovery of capabilities and sensor management. The ISA has been tested and integrated with multiple sensors, platforms, and over a variety of hardware architectures in operational environments.

Keywords: interoperability, live virtual constructive, disadvantaged network, sensor

1. INTRODUCTION

In 2003 the Networked Sensors for the Future Force (NSFF) Advanced Technology Demonstration (ATD) effort was created to dynamically integrate multiple live, virtual, and constructive simulations with a quad reconnaissance vehicle. The effort concluded with the successful collaboration of multiple ground and aerial sensor platforms with their virtual equivalents to create a robust operational environment. During the integration effort, both the unique problems of working in tactical environments and the need for specialized approaches were identified.

1.1 Tactical Networks

Fielded operations rarely operate under the optimal conditions found in a laboratory as they are constrained by the hardware and networking infrastructure available to them. These tactical environments, otherwise known as Disconnected Intermittent and Limited (DIL) networks, are defined as those that are low bandwidth, unreliable, and constrained in some manner. To operate reliably on such a network requires the definition of protocols and behaviors that guarantee the delivery of required messages and perform a best-effort for the others. Systems must be capable of self-configuration and dynamic discovery but also able to function when disconnected from the network.

For NSFF the solution for these problems consisted of a hub and spoke architecture where nodes were connected by reliable UDP. Messages pertaining to your connection on the network and others explicitly marked important were guaranteed to be published to consumers while the other messages could possibly be lost in transit. A publication-only, high-bandwidth connection was available for enterprise connections that would receive all published data. This solution worked well for the situation it was deployed in but it would be infeasible to scale to much larger networks.

1.2 Netted Sensors

Historically military specifications for sensor systems focus primarily on performance characteristics that can directly impact battlefield situations. Interoperability, the ability of a system to easily work with other systems, is not specified at the same level of detail and it is common for sensors to rely on serial and other communication technologies that are

not network ready. When required to be network enabled, the lack of detail in the specification allows for sensors that comply with standards but still not be interoperable.

For example, industry has defined several methods for data transport and while some are well defined such as UDP and TCP, others are more loosely defined like R-UDP (a variation of reliable UDP). These are all common standards but they do not necessarily communicate with each other. In the case of R-UDP there can be multiple different designs that all fall under the same name but don't interoperate. Additionally, as there is no commonly accepted standard for protocols or data specifications, sensors often use custom solutions designed for the precise problem space of the sensor. When an attempt is made to combine these systems the outcome is a patchwork of integration efforts and expended time that frequently results in a stovepipe solution - literally one that solves that particular problem but is useless in all other circumstances.

Rather than developing many interfaces between the components on the network, the NSFF team designed a common data model that all systems would interact with. This first generation data model was very limited in the data and sensor types it could represent but it was capable of proving the cost benefit of a single standard for integration.

2. Integrated Sensor Architecture

ISA is the culmination of our efforts to build the perfect environment that solves these problems and allows for the seamless integration of producers and consumers. All systems on the network, whether they are sensors, services, or consumers, are true ISA components that are required to register, maintain state, and publish their capabilities.

2.1 ISA Services

A system of systems approach is utilized to take advantage of the dynamic nature of the network and ensure that the network will function to the best of its abilities, even in a standalone mode. Within a system multiple core services have been identified as essential to provide minimal functionality.

- Authentication - Authenticates the identity of other components to allow them to join the network.
- Registration - Monitors the connectivity of other components that have joined the network.
- Routing - Allows communications between different components on the ISA network by routing messages to the correct destination.

In addition to the core services a number of common support services have been identified. These services provide functionality to the system that are often useful in deployments.

- Authorization - Confirms permission for components to perform action on the network or other components.
- Discovery - Provides a mechanism for finding components on the network.
- Subscription - Provides a mechanism for filtered data distribution.

While some services have been identified as needed or recommended in a standard deployment, the set of services is not restricted to the provided list and it is expected that other services will arise as needed.

2.2 Common Data Standard

After years of field experimentation with a variety of sensors, systems and services the ISA team has developed a data model that is representative of the types of data exchanged between the producers and consumers. Experience gained from using other sensor data models also heavily influenced the development of the ISA model. Existing models tended to fall in one of two categories - either too rigid or too flexible. A data model that is too rigid does not allow for easy extension when unanticipated information must be exchanged. It is common practice in models of this type to either provide a catch-all structure that can be used for anything or overload an existing structure for use in a new way. In either approach the definition of the model loses meaning and the receiver can not be certain of the senders intention. On the other side of the spectrum are the extremely flexible data models. These models provide multiple ways to convey information so that the publisher is not constrained and can send information in the most native way possible. This model places a burden on the receiver, which must be prepared to handle data that comes in a variety of formats. If the

model allows temperature to be delivered in Celsius, Fahrenheit, or Kelvin, it then places a burden on the data consumer to be able to handle any of these units.

ISA takes a blended approach to the definition of the data model and attempts to capture the benefits of each approach while avoiding the pitfalls. The model provides structures for the types of data that sensors produce but limits the type of units used within the model. For example, distance can only be expressed in meters and temperature can only be expressed in Celsius. If a producer or a consumer needs another unit it is the responsibility of that component to convert from the known data type to the custom one needed internal to the component. The names of data fields are also defined so the information will be placed in a known location. The Battery field is where the current battery level is placed, and the Position field is where the current geographic position is placed. This is the rigid part of the data model that allows producers to know where to place the information and consumers know where to get it.

Flexibility is another hallmark of a solid data model. ISA accomplishes this using two features: freedom in defining new data fields and freedom in defining new data types. Within some of the top-level messages in ISA it is possible to easily add data fields that use existing data types. If the data model does not provide a sufficient data structure it is possible to define a new structure. The difference between ISA and many other data models is there are mechanisms in place that allow the component to publish the definition of the new data type. By providing the definitions of the custom data types the producer allows consumers to adjust as necessary to make full use of the data.

2.3 Standard Message Set

Throughout the ISA life cycle there are six major message types: registrations, configurations, statuses, events, requests, and responses used by a component. These messages provide a context to the information that is exchanged between the components.

Registration messages are used when a component communicates with a registrar service to establish or terminate a connection to the ISA network.

Configuration messages are used to communicate the capabilities of the component to the ISA network. Contained in this message is the current configuration of the component containing the properties it publishes, the commands it supports, and the information that it can observe. This message is the most useful for discovering components that can fulfill specific mission needs.

A status message contains current information about the component itself using a collection of property fields. Each property relays information about a specific aspect of the component. Examples of properties are the operating state, position, and battery. To minimize bandwidth usage a status message only reports when a field has changed and reports only those properties that have changed.

An event message contains information that the component has observed. The message contains the information about the observation that can be useful to other components on the network. The observed information can range from temperature measurements to locations of hostile forces depending on the nature of the component creating the message.

Request and response messages are used when commanding a component to perform an action. The component that desires the action will create a request message and send it to the performing component. After the component receives the request it will perform the action if permitted and respond with the results of the action. The results could be a code denoting success or failure, or a value if a calculation is permitted. Every component that receives a request must generate a response.

This standard messages set helps to frame the communication between components by providing a context to the information being exchanged. Without this initial context it is difficult to determine the meaning when the same data structure is used to convey different forms of information.

2.4 Security

While information assurance and security are uniformly considered essential in DoD programs, they are rarely implemented while a system is being designed. Adding such measures afterwards can be a costly and potentially complex problem. The ISA team has worked with our Information Assurance group from the beginning to ensure that this specification conforms to all recommended security practices.

ISA utilizes X.509 Public Key Infrastructure (PKI) technology to restrict access and authorize capabilities on the network. Each system must present a valid certificate and negotiate an encrypted connection to the controller it connects with and that controller will verify those credentials prior to allowing access.

In such an infrastructure each component will have a public / private key pair and they will share the public key with others they connect to. This public key acts as both a secure identifier of the component and as a means to encrypt data that only that component can decrypt. Each of these keys is signed by at least one Certificate Authority (CA) and a list of trusted CAs can be generated to build up a web of trusted keys on a network. This web of trust can either be dynamically queried for or pre-loaded on a mission by mission basis.

2.5 Network Topology and Protocols

Building upon the lessons learned from the initial and subsequent iterations, the ISA infrastructure uses a mesh topology and multiple connection protocols as determined by the specific operating environment. Dynamic negotiation of the application encoding is possible but most of the current implementations use an encoding based upon Google's Protocol Buffers.

Within a DIL environment the recommended setup uses Stream Control Transmission Protocol (SCTP) as the transport layer and Datagram Transport Layer Security (DTLS) for the session and security. SCTP is a datagram protocol that allows for multiple streams of data with different qualities of service for each and allows, when needed, for reliable data transmission over an unreliable network. The DTLS layer provides the necessary security and authorization framework over such a connection. This combination allows for a secure and robust connection over a suboptimal network.

On a more robust tactical connection the recommended setup is to use Transmission Control Protocol (TCP) as the transport and Transport Layer Security (TLS) for the session and security. While this combination is less optimal over disadvantaged networks, and we do not recommend it there, TCP and TLS perform adequately over networks with relatively minor loss and it is far more common to find developers who are familiar with these protocols than the more recently developed SCTP and DTLS.

When operating on a highly-available, high-bandwidth network, frequently referred to as an enterprise connection, a typical connection would be over a web-based Representation State Transfer (REST) connection protected by TLS security.

Regardless of how a component connects into the ISA network, all components will have the same basic data set and behaviors and are able to seamlessly interact with other ISA members.

2.6 Component Capabilities Description (CCD)

A critical concept to the ISA component model is the CCD which every component must publish upon registering with the ISA network. The CCD describes the data properties that the component will publish about itself, the commands that can be executed upon it, the observable data elements that will be published in events generated by this component, and any custom data types that are used. This fully defines what is needed to interact and understand a new component that registers on the network.

The ISA capabilities document defines the standard set of properties, commands, and observables associated with a particular component modality. For example, all gimbal devices are expected to implement slew and point commands and all subscription services implement a set of commands that will provide data to consumers. Even though these are only guidelines for how these components should represent themselves they are an important facets of the system in order to provide seamless interoperability between components. Without such guidelines, every component on the network would ~~have to have~~ require pre-existing knowledge about the capabilities of other components it discovers in order to work with them.

2.7 Interoperability Levels

ISA defines multiple levels of interoperability between a component and the system. These levels do not define the degree of compliance with the specification but more the type of interactions that will occur between components.

Level 1 interoperability is defined as sending and receiving data through agents using an asynchronous publication and subscription mechanism. This level is the bare minimum required to be a valid component on the network and requires

the component to register, send their configuration, and update their status, and generate events as needed. These components are not required to understand the complexities of the network topology and will only directly interact with the controller they are registered with.

Level 2 interactions build upon those of Level 1 with the addition of commands and responses. This interoperability level expects that the component will implement commands that can be acted upon by an outside agent to produce changes in the properties and behaviors of that component. In a typical deployment, these commands will be executed by an intelligent agent according to an operational mission. Direct commanding of another component is possible; however, depending on deployment and the individual systems requirements, this would be restricted and controlled by the authorization service.

A Level 3 connection is a direct, bi-directional interface to another component without any intervening agents. After connecting to an ISA network, the component may be able to discover an asset that it would prefer to connect to outside of the ISA network. This connection would be through a natively-encoded direct connection. The component is required to manage that connection entirely on its own and, at the same time, persist its connection with the ISA network. The advantage of a Level 3 direct connection is apparent in situations where there is a pre-existing interface between two systems that provides functionality not currently available through ISA.

3. Live Virtual Constructive (LVC) Environments

ISA is capable of operating in an LVC environment. Typically, LVC environments depend on translators and middleware to achieve seamless data transfer between the virtual and live assets. This process is limited in its ability to interact with the live assets, causing the constructive simulation to be limited by the translators and middleware. Having ISA enabled components connected to a simulation network would allow for seamless integration of the live and simulated sensors with no additional overhead or latency between components. Using the ISA levels of interoperability, the live and virtual comments would be able to share information and tasking, allowing for a more robust simulation. The ease in which ISA components can be brought on the LVC environment allows for faster integration and testing with the simulated assets. With the addition of ISA, sensors to the LVC environment testing can be conducted over tactical networks for live sensor load testing. Also, the distributed simulation events could be conducted that show the affects of loading on the live sensors, as well as possible deployment and policy implications of new technology. The ISA can be used to easily and dynamically integrate live and virtual sensors that allow for different configurations and systems to be used for LVC testing.

4. Future Directions

The ISA specification has been designed to be both robust and relatively lightweight, with the intention that it could be implemented both on existing hardware and systems without impacting their operations. To date we have deployed our complete reference implementation on systems as small as an Android cell phone or Raspberry Pi.

Future ISA work will focus on improving the underlying mesh infrastructure to maximize efficiency and quality of service to sensors and systems. Additionally, more complex services will be implemented to enhance the initial capabilities and better anticipate the needs of a component. The computational overhead of ISA may also be further optimized to make it an attractive solution for live virtual constructive environments (LVC) that can be embedded directly into sensor hardware.

Conclusion

The Integrated Sensor Architecture is an interoperability solution that allows for the sharing of information between sensors and systems in a dynamic tactical environment. The ISA created a Service Oriented Architecture that identifies

common standards and protocols which support a net-centric system of systems integration. Utilizing a common language, these systems are able to connect, publish their needs and capabilities, and interact with systems. Extensible data models and capabilities that are scalable across multi-echelons are supported, as well as dynamic discovery of capabilities and sensor management. The ISA has been tested and integrated with sensors, platforms, and hardware architectures. ISA allows for net-centric systems to share information in a distributed environment that enables seamless connections between virtual and live systems. This would allow for improved distributed testing and simulations.